REMARKS

The courtesy of Examiner Gurshman and Smithers in granting an interview on August 12, 2003, as reflected by the Interview Summary of that date, is acknowledged and greatly appreciated.

The foregoing amendments to independent claims 1, 9, 18, 19, 22, 26, 27, 28, 29, 30 and 31 are respectfully submitted to be pursuant to and consistent with an agreement reached at the interview, namely, these amendments to those claims correspond to amendments of claims 17 and 25 presented in the Preliminary Amendment filed by Certificate of Mailing dated July 21, 2003, an informal copy of which was discussed at the aforesaid interview. Applicants' counsel understood from the interview that claims 17 and 25 were considered to patentably distinguish over the art of record. Applicants also incorporate herein the arguments distinguishing over the art of record as set forth in the Preliminary Amendment.

The amendments introduced to the above-specified claims, moreover, delineate as between converted biometric information (and variations thereof, including converted and extracted feature biometric information, and the reverse sequence of those functions) being currently obtained for a specific individual and being compared with the same such information previously obtained and registered, in advance, for purposes of authenticating the individual. (The precise recitations, of course, should be considered, as they appear in the individual claims.)

CONCLUSION

In accordance with the foregoing, it is respectfully submitted that the claims patentably distinguish over the art of record and, there being no other objections or rejections, that the application is in condition for allowance, which action is earnestly solicited.

ERRATA IN PRELIMINARY AMENDMENT

At the interview, applicants noted certain errors appearing in the aforesaid Preliminary Amendment and, at the interview, errata sheets, bearing hand-written annotations correcting those errors, were presented at the interview but were not filed at that time.

Accordingly, attached are the errata sheets and corrected pages for substitution in the Preliminary Amendment, as filed, correcting the errors.

Approval and entry of the errata sheets are respectfully requested.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 2, 2003

By: _____

H. J. Staas
Registration No. 22,010

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

ERRATA: PRELIMINARY AMENDMENT

BY COMMUNICATION ON JULY 21, 2003

PAGE 2 AND 1-13

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered). Please AMEND claims, and ADD new claims, in accordance with the following:

1. (ORIGINAL) An authentication apparatus comprising:

measuring means for measuring biometric information of an individual;

converting means for carrying out a predetermined conversion process with respect to the biometric information so as to obtain converted biometric information;

extracting means for extracting feature information from the converted biometric information so as to obtain extracted feature information; and

verifying means for verifying the extracted feature information with respect to registered information which is registered in advance, so as to authenticate the individual.

2. (CURRENTLY AMENDED) The authentication apparatus as claimed in claim ~~1~~ 2, which further comprises:

input means for inputting parameters used by said converting means for the predetermined conversion process.

3. (CURRENTLY AMENDED) The authentication apparatus as claimed in claim ~~1~~ 2, wherein said converting means uses personal information related to the individual as the parameters.

4. (CURRENTLY AMENDED) The authentication apparatus as claimed in claim ~~1~~ 2, wherein said verifying means receives the registered information by a communication which is made via a medium, and said converting means uses an enciphering key which is used for the communication as the parameters used for the predetermined conversion process.

5. (ORIGINAL) The authentication apparatus as claimed in claim 1, wherein the

REMARKS

In accordance with the foregoing, pending claims 3, 4, 11 and 12 are amended to correct claim dependencies thereof, claims 17 and 25 are amended to introduce a further aspect of a "verifying" function in accordance with the invention and new claims 31-33 are added, all as discussed more fully hereinafter. No new matter is presented and, accordingly, approval and entry of the amended and new claims are respectfully requested.

THE PRESENT INVENTION

As discussed in further detail in the intervening response, the remarks of which are incorporated herein by reference, the present invention carries out verification by comparing (a) a feature extracted from converted biometric information or, (b) a feature which is first extracted from the biometric information and then converted or, (c) the converted biometric information, with respect to the registered information, so as to authnenticate an individual. Because the verification is made by directly comparing the converted information (a) or (b) or (c) with respect to the registered information, the original biometric information cannot be stolen when carrying out the verification. Even if a third party steals the converted information (a) or (b) or (c), the original biometric used for the conversion ~~are~~ cannot be stolen.

Even if it assumed for the sake of argument that the parameters used for the conversion were somehow stolen, the parameter used for the conversion may simply be changed thereafter. When the parameters used for the conversion are changed to new parameters, neither the stolen, previously converted information nor the stolen, original biometric information can be verified, because the verification is now made using the converted information (a) or (b) or (c) which is obtained by conversion using the new parameters. In addition, the original biometric information does not need to be changed for maintaining the security of same, because the original biometric information is now converted using the new parameters.

THE PRESENT INVENTION, AS CLAIMED, PATENTABLY DISTINGUISHES OVER THE REFERENCES OF RECORD

These foregoing advantageous effects of the present invention cannot be obtained in either Kanevsky and Priddy, because both require the encrypted or encoded biometric

information to be decrypted or decoded before the comparison is made with the registered biometric information for performing verification. For this reason, the decrypted or decoded biometric information, that is, the original biometric information, is vulnerable to theft or other misuse when carrying out the verification. If this original biometric information is stolen, the stolen biometric information may be used improperly, i.e., without authorization, for the verification. In addition, if it is discovered that the biometric information has been stolen, the biometric information, to be used for verification, must be changed to reinstate security. But since the amount of biometric information is limited, it may be very difficult to correct for the theft of biometric information in some cases, such as the case where the user's iris is used to change the stored biometric information to be used for the verification.

To the extent the Examiner may be confusing the "key" used in encryption and description with "parameters" used for their conversion in the present invention, changing the "key" will not help solve the problem described above. Even if the "key" is changed, it is still necessary to decrypt the encrypted biometric information, for comparison with the registered biometric information, in order to carry out the verification. Hence, it is still necessary to change the biometric information to be used for the verification for security when the biometric information is stolen.

Furthermore, it should also be noted that, if someone capable of accessing a server system which manages the registered information (biometric information) of Kanevsky wishes to steal the biometric information, it is also possible to steal the registered (stored) biometric information instead of the decrypted biometric information. On the other hand, even if the registered information (converted biometric information) of the present invention is stolen, the converted biometric information is meaningless unless the parameters used for the converted are known, as explained above.

In paragraph 2 on page 2 of the Office Action, the Examiner acknowledges that an important feature of the claimed invention is the "conversions" of the original biometric information. However, the Examiner assets, incorrectly, that this important feature is taught in Kanevsky and also in the newly cited reference to Priddy.

First, the "conversion" used in the present invention is not the same as the "encryption" of the Kanevsky, because the encrypted data in Kanevsky cannot be used for a subsequent process unless decrypted, as will be explained later. Even if one were to assume, for the sake of argument, that the foregoing "conversion" and "encryption" were comparable, the present

invention still is clearly different from Kanevsky. As explained in the previous response filed January 21, 2003, Kanevsky cannot carry out a verifying process using the encrypted data as it is; instead, Kanevsky must decrypt the encrypted data back to the original form in order to carry out the verifying process.

With regard to Priddy, col. 7, lines 33-35 cited by the Examiner merely mentions encoding of the biometric data. However, the "encoding" of Priddy may be regarded to be similar to the "encryption" of Kanevsky and, thus, is no more relevant to the present claimed invention than Kanevsky. As in the case of Kanevsky, Priddy cannot carry out a verifying process using the encoded data as it is and, instead, must decode the encoded data back to the original form in order to carry out the verifying process.

In paragraph 3 on page 2 of the Office Action, the Examiner correctly characterizes two basic elements, or functions, of the present invention, as recited in claims 1-8 and 19-21, wherein biometric information is first converted and then feature information is extracted from the converted biometric information. However, the Examiner fails to consider another important element, or function, of the present invention, namely, the verification, recited in the closing paragraph of each of claims 1 and 19. Particularly, the present invention verifies the extracted feature information (which is extracted from the converted biometric information) with respect to registered information which is registered in advance, so as to authenticate the individual. Kanevsky presents no such teaching or suggestion.

Indeed, in paragraph 3, the Examiner merely asserts that:

> ...Kanevsky teaches first encrypting the information and then creating an encrypted print (feature information) see Fig. 2, blocks 200, 202, 204.

The Examiner's contention not only ignores the claimed verification means and functions respectively of claims 1 and 19, the cited blocks 200, 202 and 204 in Fig. 2 of Kanevsky and the corresponding description, in fact, are completely unrelated to the present, claimed invention, as recited in claims 1-8 and 19-21. Kanevsky merely encrypts the extracted biometric information, transmits the encrypted and extracted biometric information, decrypts the received encrypted extracted biometric information, and compares the decrypted extracted biometric information with registered information for verification. Kanevsky thus is subject to the very deficiencies of the prior art with regard to security issues, which the present invention overcomes, contrary to the Examiner's contention in the preceding paragraph 2 on page 2 of the Action.

In paragraph 4 on pages 2-3 of the Office Action, the Examiner correctly characterizes the present invention, as recited in claims 9-16 and 22-24, wherein the feature information is first extracted from the biometric information then the extracted feature information is converted. However, the Examiner again fails to consider the important further element, or function, of the present invention, namely, the verifying process. Particularly, the present invention verifies the converted, extracted feature information (which is obtained by converting the feature information extracted from the biometric information) with respect to registered information which is registered in advance, so as to authenticate the individual.

Col. 4, line 15 and col. 6, line 5 of Kanevsky are completely unrelated to the present invention, as recited in claims 9-16 and 22-24. Kanevsky merely encrypts the extracted biometric information, transmits the encrypted extracted biometric information, decrypts the received encrypted extracted biometric information, and compares the decrypted extracted biometric information with registered information for verification.

Paragraph 5 on page 3 of the Office Action relates to claims 27-30, ~~newly added~~ in the prior response and which claims ~~27-30~~ now are rejected for anticipation under 35 USC § 102(e) by a newly cited reference to Priddy, in paragraphs 13-14 on page 5 of the Office Action. Accordingly, applicants respond thereto subsequently in this response.

Further, paragraph 6 on page 3 of the Office Action rejects the newly added claims 27-30 for anticipation under 35 USC § 102(e) by Kanevsky, in paragraphs 8 and 12 and to which applicants respond hereinafter.

In paragraphs 8-12 on pages 3-4 of the Office Action, claims 1-16 , 18-24 and 26-30 are rejected under 35 USC § 102(e) as being anticipated by Kanevsky.

The rejections are respectfully traversed.

As explained above, Kanevsky fails to teach or even suggest the present invention, as recited in claims 1-8, 19-21, 27 and 29, wherein the biometric information is first converted and then the feature information is extracted, and the extracted feature information (which is extracted from the converted biometric information) is verified with respect to registered information which is registered in advance, so as to authenticate the individual.

Further, as also explained above, Kanevsky fails to teach or even suggest the present invention, as recited in claims 9-16, 22-24, 28 and 30, wherein the feature information is first extracted from the biometric information then the extracted feature information is converted, and

ERRATA: CORRECTED FORMAL PAGES

2 AND 1-13 FOR REPLACEMENT IN

PRELIMINARY AMENDMENT FILED JULY 21, 2003

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered). Please AMEND claims, and ADD new claims, in accordance with the following:

1. (ORIGINAL) An authentication apparatus comprising:

measuring means for measuring biometric information of an individual;

converting means for carrying out a predetermined conversion process with respect to the biometric information so as to obtain converted biometric information;

extracting means for extracting feature information from the converted biometric information so as to obtain extracted feature information; and

verifying means for verifying the extracted feature information with respect to registered information which is registered in advance, so as to authenticate the individual.

2. (ORIGINAL) The authentication apparatus as claimed in claim 1, which further comprises:

input means for inputting parameters used by said converting means for the predetermined conversion process.

3. (CURRENTLY AMENDED) The authentication apparatus as claimed in claim ~~1~~ 2, wherein said converting means uses personal information related to the individual as the parameters.

4. (CURRENTLY AMENDED) The authentication apparatus as claimed in claim ~~1~~ 2, wherein said verifying means receives the registered information by a communication which is made via a medium, and said converting means uses an enciphering key which is used for the communication as the parameters used for the predetermined conversion process.

5. (ORIGINAL) The authentication apparatus as claimed in claim 1, wherein the

REMARKS

In accordance with the foregoing, pending claims 3, 4, 11 and 12 are amended to correct claim dependencies thereof, claims 17 and 25 are amended to introduce a further aspect of a "verifying" function in accordance with the invention and new claims 31-33 are added, all as discussed more fully hereinafter. No new matter is presented and, accordingly, approval and entry of the amended and new claims are respectfully requested.

THE PRESENT INVENTION

As discussed in further detail in the intervening response, the remarks of which are incorporated herein by reference, the present invention carries out verification by comparing (a) a feature extracted from converted biometric information or, (b) a feature which is first extracted from the biometric information and then converted or, (c) the converted biometric information, with respect to registered information, so as to authnenticate an individual. Because the verification is made by directly comparing the converted information (a) or (b) or (c) with respect to the registered information, the original biometric information cannot be stolen when carrying out the verification. Even if a third party steals the converted information (a) or (b) or (c), the original biometric used for the conversion cannot be stolen.

Even if it assumed for the sake of argument that the parameters used for the conversion were somehow stolen, the parameters used for the conversion may simply be changed thereafter. When the parameters used for the conversion are changed to new parameters, neither the stolen, previously converted information nor the stolen, original biometric information can be verified, because the verification is now made using the converted information (a) or (b) or (c) which is obtained by conversion using the new parameters. In addition, the original biometric information does not need to be changed for maintaining the security of same, because the original biometric information is now converted using the new parameters.

THE PRESENT INVENTION, AS CLAIMED, PATENTABLY DISTINGUISHES OVER THE REFERENCES OF RECORD

These foregoing advantageous effects of the present invention cannot be obtained in either Kanevsky and Priddy, because both require the encrypted or encoded biometric information to be decrypted or decoded before the comparison is made with the registered

biometric information for performing verification. For this reason, the decrypted or decoded biometric information, that is, the original biometric information, is vulnerable to theft or other misuse when carrying out the verification. If this original biometric information is stolen, the stolen biometric information may be used improperly, i.e., without authorization, for the verification. In addition, if it is discovered that the biometric information has been stolen, the biometric information, to be used for verification, must be changed to reinstate security. But since the amount of biometric information is limited, it may be very difficult to correct for the theft of biometric information in some cases, such as the case where the user's iris is used to change the stored biometric information to be used for the verification.

To the extent the Examiner may be confusing the "key" used in encryption and description with "parameters" used for their conversion in the present invention, changing the "key" will not help solve the problem described above. Even if the "key" is changed, it is still necessary to decrypt the encrypted biometric information, for comparison with the registered biometric information, in order to carry out the verification. Hence, it is still necessary to change the biometric information to be used for the verification for security when the biometric information is stolen.

Furthermore, it should also be noted that, if someone capable of accessing a server system which manages the registered information (biometric information) of Kanevsky wishes to steal the biometric information, it is also possible to steal the registered (stored) biometric information instead of the decrypted biometric information. On the other hand, even if the registered information (converted biometric information) of the present invention is stolen, the converted biometric information is meaningless unless the parameters used for the conversion are known, as explained above.

In paragraph 2 on page 2 of the Office Action, the Examiner acknowledges that an important feature of the claimed invention is the "conversions" of the original biometric information. However, the Examiner assets, incorrectly, that this important feature is taught in Kanevsky and also in the newly cited reference to Priddy.

First, the "conversion" used in the present invention is not the same as the "encryption" of the Kanevsky, because the encrypted data in Kanevsky cannot be used for a subsequent process unless decrypted, as will be explained later. Even if one were to assume, for the sake of argument, that the foregoing "conversion" and "encryption" were comparable, the present invention still is clearly different from Kanevsky. As explained in the previous response filed

January 21, 2003, Kanevsky cannot carry out a verifying process using the encrypted data as it is; instead, Kanevsky must decrypt the encrypted data back to the original form in order to carry out the verifying process.

With regard to Priddy, col. 7, lines 33-35 cited by the Examiner merely mentions encoding of the biometric data. However, the "encoding" of Priddy may be regarded to be similar to the "encryption" of Kanevsky and, thus, is no more relevant to the present claimed invention than Kanevsky. As in the case of Kanevsky, Priddy cannot carry out a verifying process using the encoded data as it is and, instead, must decode the encoded data back to the original form in order to carry out the verifying process.

In paragraph 3 on page 2 of the Office Action, the Examiner correctly characterizes two basic elements, or functions, of the present invention, as recited in claims 1-8 and 19-21, wherein biometric information is first converted and then feature information is extracted from the converted biometric information. However, the Examiner fails to consider another important element, or function, of the present invention, namely, the verification, recited in the closing paragraph of each of claims 1 and 19. Particularly, the present invention verifies the extracted feature information (which is extracted from the converted biometric information) with respect to registered information which is registered in advance, so as to authenticate the individual. Kanevsky presents no such teaching or suggestion.

Indeed, in paragraph 3, the Examiner merely asserts that:

> ...Kanevsky teaches first encrypting the information and then creating an encrypted print (feature information) see Fig. 2, blocks 200, 202, 204.

The Examiner's contention not only ignores the claimed verification means and functions respectively of claims 1 and 19, the cited blocks 200, 202 and 204 in Fig. 2 of Kanevsky and the corresponding description, in fact, are completely unrelated to the present, claimed invention, as recited in claims 1-8 and 19-21. Kanevsky merely encrypts the extracted biometric information, transmits the encrypted and extracted biometric information, decrypts the received encrypted extracted biometric information, and compares the decrypted extracted biometric information with registered information for verification. Kanevsky thus is subject to the very deficiencies of the prior art with regard to security issues, which the present invention overcomes, contrary to the Examiner's contention in the preceding paragraph 2 on page 2 of the Action.

In paragraph 4 on pages 2-3 of the Office Action, the Examiner correctly characterizes the present invention, as recited in claims 9-16 and 22-24, wherein the feature information is first extracted from the biometric information then the extracted feature information is converted. However, the Examiner again fails to consider the important further element, or function, of the present invention, namely, the verifying process. Particularly, the present invention verifies the converted, extracted feature information (which is obtained by converting the feature information extracted from the biometric information) with respect to registered information which is registered in advance, so as to authenticate the individual.

Col. 4, line 15 and col. 6, line 5 of Kanevsky are completely unrelated to the present invention, as recited in claims 9-16 and 22-24. Kanevsky merely encrypts the extracted biometric information, transmits the encrypted extracted biometric information, decrypts the received encrypted extracted biometric information, and compares the decrypted extracted biometric information with registered information for verification.

Paragraph 5 on page 3 of the Office Action relates to claims 17 and 25, once amended in the prior response and which claims now are rejected for anticipation under 35 USC § 102(e) by a newly cited reference to Priddy, in paragraphs 13-14 on page 5 of the Office Action. Accordingly, applicants respond thereto subsequently in this response.

Further, paragraph 6 on page 3 of the Office Action rejects the newly added claims 27-30 for anticipation under 35 USC § 102(e) by Kanevsky, in paragraphs 8 and 12 and to which applicants respond hereinafter.

In paragraphs 8-12 on pages 3-4 of the Office Action, claims 1-16 , 18-24 and 26-30 are rejected under 35 USC § 102(e) as being anticipated by Kanevsky.

The rejections are respectfully traversed.

As explained above, Kanevsky fails to teach or even suggest the present invention, as recited in claims 1-8, 19-21, 27 and 29, wherein the biometric information is first converted and then the feature information is extracted, and the extracted feature information (which is extracted from the converted biometric information) is verified with respect to registered information which is registered in advance, so as to authenticate the individual.

Further, as also explained above, Kanevsky fails to teach or even suggest the present invention, as recited in claims 9-16, 22-24, 28 and 30, wherein the feature information is first extracted from the biometric information then the extracted feature information is converted,